REMARKS

Claims 1-10, 12-19, 21-28, and 31-38 are pending. Claims 1, 10, 18, 23, and 25 are in independent form.

In the action mailed December 7, 2005, the drawings filed on February 7, 2006 were objected to. Upon review, it appears that annotated sheets of drawings were incorrectly labeled as "replacement" sheets. Applicant apologizes for the error. Also, it appears that the replacement sheets of formal drawings filed that same day and now available at the USPTO PAIR site are very poor copies.

Accordingly, submitted herewith is another, correctly labeled, copy of the replacement sheets of formal drawings. Applicant thanks the Examiner for the attention to this matter.

Claims 18, 19, 21, 22, and 32 have been allowed and claims 2, 3, 5-8, 12-15, 24, 26, and 27 have been indicated as containing patentable subject matter. The indication of patentable subject matter is gratefully acknowledged.

CLAIMS 1 and 23

Claims 1 and 23 were rejected under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 6,754,349 to Arthan (hereinafter "Arthan").

Claim 1 relates to a method that includes defining a key and a set of values, sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage, and sending a second value of the set, but not all of the values of the set to a first delegate. The key able to be derived using the values and a predefined relationship between the values. The encrypted information is accessible with the key, inaccessible with the first of the values of the set absent the second of the values of the set, and inaccessible with the second of the values of the set absent the first of the values of the set.

Claim 23 relates to an article that includes a machine-readable medium that stores machine-executable instructions. The instructions are operable to cause a machine to act in accordance with claim 1.

The rejection is based on the contention that claims 1 and 23 would be obvious to one of ordinary skill in light of Arthan. Applicant respectfully disagrees.

In this regard, Arthan describes a system that recovers "key material" that has been lost or damaged at a client computer even when a network that joins the client to a key management server. *See, e.g., Arthan*, col. 1, line 6-11; col. 2, line 8-12. The "key material" can be lost or damaged due to operator error or when a removable storage device (e.g., a memory card or a floppy disk) that stores the key material is faulty. *See, e.g., Arthan*, col. 2, line 26-28.

Arthan's key management server 5 is responsible for generating and distributing cryptographic keys to the clients. *See, e.g., Arthan*, col. 2, line 6-8. When new cryptographic key material (denoted as "PRKEYS" in Arthan) is distributed from key management server 5 to a client, the client stores the new key material in a removable storage device. *See Arthan*, col. 2, line 63-67. The client also generates a random number "RSEED." *See Arthan*, col. 3, line 1-3.

This random number "RSEED" is used to compute a recovery key "RKEK" when it is hashed with the new cryptographic key material "PRKEYS." *See Arthan*, col. 3, line 6-8. This recovery key "RKEK" is in turn used to encrypt the new cryptographic key material "PRKEYS," and the encryption result is stored along with the random number "RSEED" that was used to compute recovery key "RKEK." *See Arthan*, col. 3, line 10-15. Recovery key "RKEK" is then erased from the client. *See Arthan*, col. 3, line 16-21.

When the new cryptographic key material "PRKEYS" stored on the removable storage device becomes unavailable at the client, a human at the client calls a human at the key management server and dictates the random number "RSEED" that was stored on at the client. *See Arthan*, col. 3, line 24-44. The key management server can recalculate the recovery key "RKEK" by hashing the random number "RSEED" with the (formerly) new cryptographic key material "PRKEYS." *See Arthan*, col. 3, line 44-46.

The human at the key management server then dictates the recalculated recovery key "RKEK" to the human at the client, who in turn can use the recovery key "RKEK" to recover the (formerly) new cryptographic key material "PRKEYS" by decrypting the encryption of new cryptographic key material "PRKEYS" by the recovery key "RKEK." *See Arthan*, col. 3, line 53-59.

As best understood by applicant, the rejection contends that the new cryptographic key material "PRKEYS" is sent by Arthan's client to key management server 5. *See Office Action*, page 3, line 7-9.

Applicant respectfully disagrees. As discussed above, the new cryptographic key material "PRKEYS" (i.e., the secret of Arthan, col. 2, line 63-64) is generated by the key management server 5 and sent to the client. Arthan neither describes nor suggests that "PRKEYS" is ever sent to key management server 5. Moreover, since key management server 5 generates the PRKEYS, the sending of PRKEYS from Arthan's client to key management server 5 would not be obvious to one of ordinary skill. Accordingly, Arthan neither describes nor suggest sending a second value of a set, but not all of the values of the set to a first delegate, as recited in claims 1 and 23.

Moreover, in contending that Arthan describes sending a first value of the set, but not all of the values of the set and information encrypted using the key to a server for storage, the rejection contends that:

-the recovery key "RKEK" constitutes "a first value of the set;"

-the new cryptographic key material "PRKEYS" encrypted with the recovery key "RKEK" constitutes "information encrypted using the key;" and

-the recovery key "RKEK" and the encrypted new cryptographic key material "PRKEYS" are sent to Arthan's client for storage.

Applicant respectfully disagrees with these assertions for several reasons. To begin with, claims 1 and 23 explicitly recite that "the encrypted information is … inaccessible with the first of the values of the set absent the second of the values of the set." However, since Arthan's new cryptographic key material "PRKEYS" was encrypted with the recovery key "RKEK," the new cryptographic key material "PRKEYS" is clearly accessible with the recovery key "RKEK." Indeed, the human at Arthan's key management server 5 dictates the recovery key "RKEK" to a human at the client for the express purpose of allowing the human to recover the new cryptographic key material "PRKEYS."

Moreover, the contention that the recovery key "RKEK" and the encrypted new cryptographic key material "PRKEYS" are sent to a Arthan's client for storage is also mistaken. The encryption of new cryptographic key material "PRKEYS" with the recovery key "RKEK" occurs at Arthan's client. Once again, the rejection contends that it would be obvious to send information to a system component where it is generated. Applicant respectfully submits that Arthan fails to describe such a sending, and moreover such a sending would not be obvious to one of ordinary skill. Accordingly, Arthan neither describes nor suggests sending a first value of a set, but not all of the values of the set and information encrypted using the key to a server for storage, as recited in claims 1 and 23.

Since elements and/or limitations recited in claims 1 and 23 are neither described nor suggested by Arthan, Applicant submits that a *prima facie* case of obviousness has not been established. Applicant respectfully requests that the rejections of claims 1, 23, and the claims dependent therefrom be withdrawn.

CLAIM 10

Claim 10 was rejected under 35 U.S.C. § 103(a) as obvious over Arthan.

Claim 10 relates to a method that includes storing, on a server accessible through a network, secured information and a first access component, excluding both the key and the second access component from storage on the server, and providing the secured information and the first access component to a first requestor. Access to the secured information requires a key. The key is able to be derived using the first access component, a second access component, and a relationship between the first and second access components.

The rejection of claim 10 is based on the contentions that Arthan's client is a server and that the new cryptographic key material "PRKEYS" constitutes the "second access component" which is excluded from storage on the server.

Applicant respectfully disagrees. Indeed, the new cryptographic key material "PRKEYS" is clearly not excluded from storage on Arthan's client. Indeed, the entire purpose of Arthan's system is to allow the client to recover the new cryptographic key material "PRKEYS" and use it in business processes. *See, e.g., Arthan*, col. 3, line 53-67.

Therefore, Arthan neither describes nor suggests excluding a second access component from storage on the server, as recited in claim 10. A *prima facie* case of obviousness has not been established, and Applicant respectfully requests that the rejections of claim 10 and the claims dependent therefrom be withdrawn.

CLAIM 25

Claim 25 was rejected under 35 U.S.C. § 103(a) as obvious over Arthan.

Claim 25 relates to an apparatus that includes a processor and instructions. The instructions are configured to cause the processor to receive, from a client, information and a value of a set of values, store the information and the value, but not all the values of the set, and transmit, to a delegate, the information and the value. The information is encrypted using a key. The key able to be derived using the values of the set and a predefined relationship between the values.

The rejection of claim 25 contends that the apparatus of claim 25 "carries out the methods of claims 1 and 9." Applicant respectfully disagrees and requests that the subject matter plainly recited in claim 25 be given proper weight.

Moreover, Applicant submits that Arthan does not render the subject matter recited in claim 25 obvious. For example, the encrypted new cryptographic key material "PRKEYS" encrypted with the recovery key "RKEK" is never received from a client, nor is it ever transmitted to a delegate, as recited in claim 25.

Accordingly, anticipation has not been established and Applicant respectfully requests that the rejections of claim 25 and the claims dependent therefrom be withdrawn.

Applicant asks that all claims be allowed. A check for the excess claims fee is enclosed. Please apply any credits or additional charges to Deposit Account No. 06-1050.

Respectfully submitted,

Date: August 14, 2006

Scott C. Harris
Reg. No. 32,030
Attorney for Intel Corporation

BY
JOHN F. CONROY
REG. NO. 45,485

Fish & Richardson P.C.
PTO Customer No. **20985**
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

SCH/JFC/jhg
10653676.doc